IN THE CLAIMS

A detailed listing of the pending claims is provided below. A status identifier is provided for each claim in a parenthetical expression following each claim number.

1. (Previously Presented) An assembly comprising:

a device physically sized in a form factor of a PCMCIA card, the device having an interface to communicate with a storage card and a flash memory to store user data; and

a removable smart card associated with a user that alternately enables access to the user data on the memory when interfaced with the device interface and disables access to the user data when removed from the device.

Claims 2 and 3: Canceled

4. (Original) An assembly as recited in claim 1, wherein the device stores a user's profile that can be used to configure a computer.

5. (Previously Presented) An assembly as recited in claim 1, wherein the smart card stores a passcode and access to the user data in the flash memory is enabled upon authentication of a user-supplied passcode to the passcode stored on the smart card.

6. (Previously Presented) An assembly as recited in claim 1, wherein the device stores a public key and the smart card stores a corresponding private key and access to the user data in the flash memory is enabled upon verification that the public key and the private key are associated.

Claims 7-21: Canceled

22. (Previously Presented) A computer system, comprising:

a computer having a PCMCIA device reader; and

a smart card secured memory assembly physically sized in a form factor of a PCMCIA card to compatibly interface with the PCMCIA device reader in the computer, the smart card secured memory assembly having data memory to store user data and a removable smart card that alternately enables access to the user data when present and disables access to the user data when removed.

23. (Original) A computer system as recited in claim 22, wherein the data memory comprises flash memory.

24. (Original) A computer system as recited in claim 22, wherein the smart card stores a passcode and is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the user data.

25. (Original) A computer system as recited in claim 22, wherein:

the smart card stores a first key;

the data memory stores a second key that is associated with the first key; and

the smart card is configured to authenticate the second key from the data memory using the first key as a condition for enabling access to the user data.

26. (Original) A computer system as recited in claim 22, wherein:

the smart card stores a passcode and a private key of a public/private key pair;

the data memory stores a public key of the public/private key pair; and

the smart card is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the private key and to authenticate the public key from the data memory using the private key as a condition for enabling access to the user data.

Claims 27-38: Canceled

39. (Previously Presented) An assembly, comprising:

a USB-compatible memory to store data files; and

a removable storage device to enable access to data files on the memory when the storage device communicatively interfaces with the memory.

40. (Previously Presented) An assembly according to claim 39, wherein the memory is a flash memory, and the data files include a user profile to configure a computer.

41. (Previously Presented) An assembly according to claim 39, wherein the storage device is to store a passcode, and access to the data files stored in the memory is enabled upon authentication of a user-supplied passcode to a passcode stored on the storage device.

42. (Previously Presented) An assembly according to claim 39, wherein the memory stores a public key and the storage device stores a corresponding private key, and access to the data files stored in the memory is enabled upon verification that the public key and the private key are associated.

43. (Previously Presented) An assembly according to claim 39, wherein the memory has a public area and a private area, wherein further the private area stores the data files.

44. (Previously Presented) An assembly according to claim 43, wherein the data files include a user profile and other data files.

45. (Previously Presented) A computer-readable medium having stored thereon a user profile and other data files, the computer-readable medium

further having computer-executable instructions causing one or more processors to:

authorize access to the data files on the computer-readable medium when the computer-readable medium is interfaced with a removable storage device; and

prohibit access to the data files on the computer-readable medium when the computer-readable medium is not interfaced with a removable storage device.

46. (Previously Presented) A computer-readable medium according to claim 45, wherein to authorize access to the data files on the computer-readable medium is to verify a passcode stored on the computer-readable medium with a passcode stored on the removable storage device.

47. (Previously Presented) A computer-readable medium according to claim 45, wherein to authorize access to the data files on the computer-readable medium is to verify that a public key stored on the computer-readable medium is associated with a public key stored on the removable storage device.

48. (Previously Presented) A computer-readable medium according to claim 45, wherein the computer-readable medium is a portable flash memory.

Claim 49: Canceled

50. (Currently Amended) An assembly, comprising:

removable means for storing data files; and

detachable means for enabling access to data files on the removable means when the detachable means communicatively interfaces with the removable means,

wherein the removable means includes a flash memory, and the data files include a user profile to configure a computer.

Claim 51: Canceled

52. (Previously Presented) An assembly according to claim 50, wherein the detachable means is to store a passcode, and access to the data files stored in the removable means is enabled upon authentication of a user-supplied passcode to a passcode stored on the detachable means.

53. (Previously Presented) An assembly according to claim 50, wherein the removable means stores a public key and the detachable means stores a corresponding private key, and access to the data files stored in the removable means is enabled upon verification that the public key and the private key are associated.